AIC's Comments to the Proposed Personal Data Protection Bill for Singapore

ABOUT THE ASIA INTERNET COALITION

The Asia Internet Coalition ("**AIC**") is an industry association founded by eBay, Google, Skype and Yahoo! incorporated in Hong Kong. One of the objects of the AIC is to support and promote public policy and regulatory frameworks that facilitate the development of national digital industry markets in the Asia Pacific region.

The AIC expresses its appreciation for the opportunity to comment on the previous consultations on the Proposed Personal Data Protection Bill (the "Bill") and on the current draft text of the Bill. As we have stated in our previous submission, we support with the objective of laying down a DP regime that seeks to create a balance between the need to protect individual's personal data against organization's need to obtain and process such data for legitimate and reasonable purposes. The AIC would like to emphasize that these equally important objectives are not necessarily conflicting and it is critical that, in language and implementation, the law ensures prevention of misuse of personal information in a manner that does not impede industry's capacity to innovate and use information for purposes that will benefit society.

In general, the AIC believes that the Bill succeeds in adopting language implementing its stated intent while incorporating substantial inputs from the previous consultations. The AIC submits the following views so that further improvements may still be made in several key areas, as follows:

1. Definitions of "News Organisation" and "News Activity".

The Bill defines "news organisation" as "*any organisation whose business, or part of whose business, consists of a news activity and which has been declared by the Minister, by notification in the Gazette, to be a news organisation for the purposes of this Act.*"

It also defines "news activity" as follows:

> *"(a) the gathering of news, or the preparation or compiling of articles or programmes of or concerning news, observations on news, or current affairs, for the purposes of dissemination to the public or any section of the public; or*
>
> *(b) the dissemination, to the public or any section of the public, of any article or programme of or concerning —*
>
> *(i) news;*

(ii) observations on news; or
(iii) current affairs"

News organisations are permitted to collect, use and disclose personal data about an individual without the consent of that individual, where the collection, use or disclosure is solely for the news organisation's news activity. This is therefore an important exception. We request clarification on the different forms of online news gathering such as aggregating news content and confirmation that websites making this kind of information available to the public are intended to be included within this exception.

Its essence should be that the collection, use and disclosure by a news organisation solely for the purposes of news activity. Gazetting is secondary, and is in our view irrelevant to the legitimacy of the activity and the necessity and desirability of the exception. We therefore propose that the words "*and which has been declared by the Minister, by notification in the Gazette, to be a news organisation for the purposes of this Act*" be deleted from the definition of "news organisation".

2. Definition of "Personal Information".

The Consultation Paper proposed that personal data be defined as follows:

"Personal Data" means information about an identified or identifiable individual; where "individual" means a natural person, whether living or deceased."

In our submission, we agreed with MICA's view that what constitutes personal data is context-specific and with continuous technological developments, would render efforts to populate a definitive list of personal data types unfeasible. We further noted that the proposed definition of personal data is based upon that used in the OECD Guidelines[1], but that while it is a good starting point, it needed updating because depending upon how it is implemented, defining personal data to broadly cover all information about an "identifiable individual" may disregard its context-specific nature and simply cover all information, regardless of whether the data controller can reasonably link the same with an individual.

The Bill now defines "personal data" as "data, whether true or not, about an individual who can be identified (a) from that data, or (b) from that data and other information to which the organisation is likely to have access." Among the reasons given for the change that the phrase "who can be identified" provides more clarity to data that is "identifiable" and that the proposed definition is one that industry is already familiar with, being largely adopted from the Model Data Protection Code ("Model Code").

[1] § 3.10

Unfortunately, the change does not fully consider context and, therefore, may still be overbroad when it considers as "personal information" all data about an individual who can be identified from that data and other information to which the organization is likely to have access. It is possible, for instance, for an organization to possess data that, with the application of sufficient technology and resource, could identify an individual, but nonetheless, in the context of its collection of data, the organization could not reasonably be expected to take the requisite steps towards identification. In such a context, the data in the hands of the organization should not be considered as "personal information".

We therefore reiterate our stand that personal data should be defined pragmatically, ***based upon the likelihood of identification***. One way of doing this is to restrict the definition to include only "information that can be certainly linked to an identified or identifiable individual" --- only when the data controller can certainly link data to an individual shall it be considered as "personal information". As such, we propose the additional inclusion of the following highlighted words - to part (b) of the definition: "… From that data when combined with other information to which the organization is likely to have access." However, it must be clear that the "reasonableness" standard refers to the methods employed (e.g., reasonableness of effort or expenses incurred considering the context of processing) and not to the certainty of identification.

3. Purpose

The stated purpose of the Bill is to govern the collection, use and disclosure of personal data by organization in a manner that recognizes both the right of individuals to protect their personal data and the need of organisations to collect, use or disclose personal data *for purposes that a reasonable person would consider appropriate in the circumstances* (emphasis supplied). While there is merit in using a reasonableness test, it may be implemented in an unduly restrictive manner or so narrowly as to preclude out-of-the-box or innovative uses that the usual person may contemplate as a result of the use of personal information.

4. Exclusion of data intermediaries

Sec. 4(2) of the Bill proposes an exclusion from its scope of data intermediaries "in respect of personal data processed by the data intermediary on behalf of another organization pursuant to a contract which is evidenced in writing." The rationale is that there may be differing degrees of control that organisations may have over personal data.

Given the vital role of internet intermediaries or online platforms play as enablers of economic growth, in the same manner as safe harbors provide limitations on liability of intermediaries for copyright infringement, safe harbors to protect internet intermediaries and online platforms from liability for third parties' actions must be provided by the Bill.

However, the language of Sec. 4(2) is quite narrow and it is not clear whether or not internet intermediaries or online platforms are covered by the exclusion. Considering that internet intermediaries and online platforms may not have any control whatsoever in the processing of personal information made by third parties, the Bill ought to clearly include them in the exclusion.

5. Applicability to the deceased

Sec. 4.4(b) exempts personal data of deceased individuals, except that provision relating to disclosure of personal data and Sec. 26 shall apply in respect of personal data of an individual who has been dead for not more than 10 years. The provision attempts to find a middle ground between (i) those who view the application of DP law to information of deceased individuals because they could affect the legitimate interests of family members and society; and (ii) those who do not favor such application because of compliance costs and practical difficulties in identifying the right representative for consent.

The AIC reiterates its position that the Bill should not cover deceased individuals at all because (a) certain rights (such as the rights of access and correction (mentioned in paragraphs 3.68 to 3.73 of the consultation paper) are so intimately tied to the data subject that they should only be exercised by the data subject itself; and (b) it is entirely possible that a deceased person may not desire family members to access or see private information–in the event of their demise.

6, Applicability to personal data with a Singapore link

In relation to Sec. 5, we suggest that MICA/IDA provide clarity on the definition of "use". As far as possible, the definition of "use" should be narrowly defined. As Singapore, seeks to be a regional hub for data centers and analytics work, an overly-broad definition would undermine ongoing efforts to encourage local innovation and attract relevant investment. The definition of use needs to clearly exclude hosting and analytics for Singapore to grow as a regional data hub.

In addition, Sec. 5(2)(a)(i) of the Bill provides that there is a Singapore link in relation to a requirement involving the collection of personal data about an individual, where "*the personal data is collected from an individual who is physically present in Singapore at the time of the collection*".

In the online world, it is often difficult (and sometimes impossible) for service providers to ascertain the physical location of a user. With globalisation and travel, the physical location of a user becomes increasingly nomadic and is no longer a static concept. Another difficulty arises when a data subject located in Singapore conducts online transactions with organisations located outside Singapore on terms of use governed by the laws of another jurisdiction. AIC

notes that the proposed extraterritorial application of DP law in Section 5(2)(a) would depart from best practice country of origin principles which would subject data controllers (rather than data subjects, in this case) to the law of the jurisdiction where the primary data center is located. In such a case, an organisation located outside of Singapore may inadvertently breach the Act in circumstances where it has no reason to believe that Singapore law applies, giving rise to practical challenges in the enforcement of Section 5(2)(a).We therefore think that Section 5(2)(a)(i) should be refined by adding a "knowledge" element on the part of the organisation collecting personal data. We propose that Section 5(2)(a) be amended by adding the following underlined words:

> "*(i) the personal data is collected from an individual who is physically present in Singapore at the time of the collection; or*
>
> *(ii) the personal data was located in Singapore at the time of the collection,*
>
> *provided that the organisation collecting the personal data knows or ought reasonably to know that the individual is physically present in Singapore or that the personal data was located in Singapore, as the case may be.*"

7. Creation of Advisory Committees/Preparation of Guidelines

With respect to the possible creation of one or more advisory committees as stated in Sec. 8, to provide advice to the Commission with regard to the performance of any of its functions under the Bill, considering the complexity involved in the analysis of the privacy implications of technology and related business models, it is best that private industry (particularly technology companies) be represented in such advisory committees. For the same reasons, private industry should also be consulted by the Commission in the preparation of any guidelines as mentioned in Sec. 28.

8. Designation of individuals by organisations to comply with Act

Sec. 13 requires organisations to designate individuals to comply with the Act. While we agree with this, we think that there needs to be clarity that this individual does not be personally liable for the organisation's compliance. Article 2.38 of the Consultation Paper makes this point clear -

> *"MICA also clarifies that responsibility for compliance with the PDPA rests with the organisation rather than the contact point specified by the organisation."*

For purposes of clarity, we propose that this be explicitly provided for in the Act. Section 13(6) of the Bill currently only states that "*the designation of an individual by an organisation … shall not relieve the organisation of any of its obligations under this Act*". We propose that an additional Section 13(7) be

added, to state as follows, similar to Section 58: "*No action, suit or other legal proceedings shall lie personally against any individual designated under subsection (3) or any individual delegated under subsection (4), for anything done (including any statement made) or omitted to be done in good faith in the course of or in connection with the performance in good faith of that individual's duties pursuant to the designation under subsection (3) or the delegation under subsection (4)*."

Article 2.38 of the Consultation Paper also specifies that "*MICA clarifies that organisations may identify officers so designated [as the appropriate contact point accountable for DP issues] by their positions or titles, instead of names of the officers.*" This is similarly absent from the Bill. We therefore propose that Sections 13(3), (4) and (5) be amended as follows:

> "*(3) An organisation shall designate one or more individuals to be responsible for ensuring that the organisation complies with this Act. Such designation may made by reference to the functions or positions or titles of individuals, instead of their names.*
>
> *(4) An individual designated under subsection (3) may delegate to another individual the duty conferred by that designation. Such delegation may made by reference to the function or position or title of the individual, instead of the name of the individual.*
>
> *(5) An organisation shall make available to the public the business contact information of each individual designated under subsection (3) or delegated under subsection (4), save that where the designation or delegation was made by reference to the function or position or title of an individual instead of the name, the organisation has no obligation to make available the names of the individuals designated under subsection (3) or delegated under subsection (4).*"

Similar amendments should also be made to Section 22(4)(b).

In addition, we would also like to reinforce that there should be no restriction to the geographical location of the individual(s) appointed by the organization to comply with the Act.

9. Access rights

Art. 2.94 of the Consultation Paper expresses MICA's opinion that "If the company has the ability to link the data to identify the individual, but has not done so, the organisation is not obliged to link the data and provide access rights to the individual to such identifiable data." The AIC believes that the Act should also make clear and explicit that the organization should not need to take any extra effort to identify an individual in order to fulfill an access request in Sec. 23.

10. Deemed Consent

In view of the strong stakeholder support for “deemed consent”, the Bill recognizes situations where an individual is deemed to have consented to the collection, use or disclosure of information. Sec. 17 explicitly provides that “[a]n individual is deemed to consent to the collection, use or disclosure of personal data by an organization for a purpose if – (a) the individual, without actually giving consent referred to in section 16, voluntarily provides the personal data to the organization for that purpose; and (b) it is reasonable that the individual would voluntarily provide the data. It was explained in the Consultation Paper that “organizations should generally state the purposes for which the personal data is collected upfront, in order to avoid misconstruing the purposes for which consent was given. Organizations should also ensure that the purposes be reasonably scoped and not overly broad”.

It is unclear whether or not, under this provision, (1) it is sufficient that an organisation states the purposes of collection or processing of personal data in an online privacy policy; (2) the continued use by an individual of an online product or service constitutes “deemed consent” , where the user is provided notice of the purposes of collection and processing of personal data through a privacy policy, contextual notices, and other forms of online notices; and (3) any “deemed consent” may be negated by claims (or subsequent finding by Commission) of “unreasonableness”. We welcome clarity from MICA on what constitutes “deemed consent”. Opening the door for multiple “unreasonableness” claims by users, who may have used services voluntarily and with the use of their informed judgment, subjects organisations to undue uncertainly from a compliance standpoint, especially since the claim may conceivably be made any time.

Finally, while we welcome a clear and broad enough definition of deemed consent, we would like to call the attention of MICA to different legitimate basis for collecting and processing personal data, other than consent. We would like to suggest a balanced approach for consent in the upcoming legislation. Consent is an important concept - one among others. As an example, the European Data Protection Directive presents consent as only one of the six legal options available to justify data processing and to allow individuals to control the scope of that processing.

One important alternative to consent is the so-called “balance of interest clause”, which justifies data processing for legitimate purposes if no overriding legitimate interest of the individual is at stake and the individual’s rights under the Directive are respected. Effective transparency requirements and the right to object ensure that the scope of the data processing remains under the individual’s control. Consent (even deemed consent) should not be required for routine processing. Many legitimate business models which are of benefit to customers and users as well as to the economy as a whole might be severely compromised if the law is unnecessarily rigid. Businesses depend on the use of personal data, in order to maintain and enlarge their customer base and effectively manage the delivery of products and services, which their customers in turn appreciate. Using consent as the only legitimate means of collecting and processing data would limit the ability of businesses. A modern

framework would recognize that data collection is necessary in the normal course of business for operations. For instance, websites need to collect data for numerous reasons such as to understand site traffic, improve site design, fraud detection, security defense, billing, determining which parts of a website are or are not being used, rendering a page in a format appropriate to the device and in the appropriate language, retrieving content data and delivering advertising or comply with auditing requirements. In addition, a business model reliant on use of data in exchange for free or subsidized content should be considered an important component of that legitimate interest, which may extend beyond the delivery of the immediate service to the user, to improve the services offered overall.

11. Fresh Consent for Different Purposes

Section 2.84 of the Consultation Paper discusses the need for "Fresh Consent for Different Purposes" and Section 22(1) of the Bill requires an organisation to inform the individual about "(a) the purposes for the collection, use or disclosure of the personal data, as the case may be, on or before collecting the personal data; (b) any other purpose of the user or disclosure of the personal data of which the individual has not been informed under paragraph (a), before the use or disclosure of the personal data for that purpose"

We agree that consumers ought to be informed and aware when their data is used for new purposes. However, we strongly submit that if an existing customer (who has already agreed and consented to terms and conditions in relation to personal data and the way in which we may notify that customer of any changes of purpose) fails to opt-out after he or she has been given a reasonable notice prior to the change in purpose, then the customer should be considered as having given consent to the change in purpose.

Such flexibility is especially important for internet and technology-based companies, which are inherently fast-moving industries. Constant innovation forms the backbone of such companies, as we constantly reinvent ways to provide our users with a more secure, smoother, and more efficient experience. Such innovation may create a new purpose for the use of personal data to which existing users will be notified of in accordance with standard practices.

For an internet service provider, with over a million customers, it is standard practice to notify customers of policy updates, or changes to terms and condition of use, through email notification and publishing the proposed change on the relevant webpage(s). In that way, the need to obtain fresh consent for a different purpose will be far less burdensome on organizations, both administratively and operationally, and user experience will be consistent with standard practice.

12. Retention of personal data.

Section 27 of the Bill requires an organisation that has used an individual's personal data to "*make a decision that directly affects the individual*", to retain

such personal data for at least one year after usage so that the individual has a reasonable opportunity to obtain access to it. The scope of this provision is very unclear, as the threshold for triggering the retention obligation is not defined.

We recommend that MICA clearly defines what it means to "directly affect" an individual. For example, if an online service provider uses personal data to select an advertisement for display to the individual, on the basis that such advertisement would be more relevant to the individual, can that be said to "directly affect" the individual? Would it make a difference if the advertisement was the direct proximate cause for the individual making a significant purchase, such as a car? This obligation could be unreasonably onerous for businesses operating at very large scales. Furthermore, a broad construction of this obligation could also be potentially inconsistent with international trends in respect of online service providers, which have in recent years been favouring shorter retention periods for at least certain types of user data.

13. Guidelines published by Commission.

Section 28 of the Bill empowers the Commission to publish guidelines on the manner in which the Commission will interpret, and give effect to, the Act. The objective of this, is to facilitate compliance with the Act.

However, Section 28(5) specifically provides that such guidelines will not be binding on the Commission. This may result in undesirable uncertainty and ambiguity as to the outcome from compliance with the guidelines. To encourage organizations to comply with guidelines published by the Commission, we would suggest that the Act explicitly state that organizations who comply with such guidelines will have immunity from prosecution in respect of actions undertaken in good faith for the purposes of such compliance.

14. Alternative dispute resolution.

Section 29 of the Bill permits the Commission to refer matters to mediation with the consent of the complainant and the organisation. It also empowers the Commission to direct a complainant to attempt to resolve his complaint with the organisation in the manner directed by the Commission. AIC thinks that these provisions is an encouraging effort to allow for alternative dispute resolution.

Having said that, our view is that there is room for industry self-regulation to play a much greater role in Singapore's personal data protection regime. We recommend that, where an industry has established a credible self-regulatory regime, the Commission should be empowered to direct complainants to rely on such regime in an appropriate case. This would also encourage industries to self-regulate and establish credible mechanisms.

15. Proportionality

Sec. 31 (2)(d) vests in the Commission the power to direct an organization to pay a financial penalty of such amount not exceeding $1 million as the Commission thinks fit. We still consider this limit to be rather high and suggest that MICA provide explicit guidance on different tiers of offences under the Bill, making clear that only in very serious instances of widescale breaches with real harm resulting should the maximum penalty be awarded. In other words, we ask that proportionality is highlighted as a guiding principle in the imposition of the penalty, such that the penalty will be proportionate to any harm caused by misuse of personal information.

16. Appeal

Sec. 31 (4) allows an appeal from any penalty imposed by the Commission. We suggest that there be guidelines on appeal in order to clarify the grounds that may support it.

We also propose that there be a mechanism to allow for the suspension of any order or direction issued by the Commission that is under appeal. Section 38(2) of the Bill provides that only orders to pay a financial penalty will be suspended pending an appeal, against either the order itself or the quantum of the penalty.

But Section 31 empowers the Commission to make various types of orders, including such directions as the Commission thinks fit to ensure compliance with the Act; directions to cease collecting, using and/or disclosing personal data in contravention of the Act; destruction of personal data collected in contravention of the Act; and to pay a financial penalty of an amount not exceeding S$1 million. Some of these orders are irreversible, such as the destruction of personal data, but can be appealed.

We would therefore suggest that the Bill should either provide for all orders by the Commission that are under appeal to be suspended, or empower the Chairman of the Appeal Panel and/or the duly-constituted Appeal Committee to grant a suspension of any order made by the Commission upon application by the appellant, where the circumstances make such a suspension just and reasonable.

Furthermore, we note that Section 39(1) of the Bill limits appeals to the High Court to points of law arising from decisions of the Appeal Committee, or decisions of the Appeal Committee as to the amounts of financial penalties. Given the relative novelty of this area of law in Singapore, we think that it would serve the interests of justice to allow appeals to the High Court on all aspects of decisions of the Appeal Committee, at least in the initial years of the Act. It would remain open to MICA to amend the Act to restrict the categories of cases that can be appealed to the High Court, if it subsequently determines that there is an unjustifiable volume of cases being appealed to the High Court.

17. Powers of investigation and inquiry.

The Eighth Schedule of the Bill sets out the powers of investigation and inquiry of the Commission and inspectors appointed under the Act. We note that paragraph 1(1) sets out the powers of the Commission and inspectors to require documents and information.

There are other provisions of Singapore law that also address production of documents and information, such as Section 20 of the Criminal Procedure Code 2010 (Act 15 of 2010). We therefore suggest that paragraph 1(1) be replaced by the following language, so as to be consistent with other existing provisions of Singapore law governing documents and information such as Section 20 of the Criminal Procedure Code:

> *"1.--(1) For the purposes of an investigation under section 33, where the Commission or an inspector considers that a document or other thing or piece of information is necessary or desirable for such investigation, the Commission or the inspector may issue a written order to any organisation in whose possession or power the document, thing or piece of information is believed to be, to require that organisation –*
>
> *(a) to produce to the Commission or the inspector such document, thing or piece of information at the time and place stated in the order; or*
>
> *(b) to give the Commission or the inspector access to such document, thing or piece of information."*

Consequential amendments would also have to be made to the other sub-paragraphs of paragraph 1.

Paragraph 2 of the Eighth Schedule empowers inspectors to enter premises without warrant, subject to certain stipulated conditions. We suggest that the Bill be amended to limit the hours of the intended entry to ordinary business hours. Otherwise, it may be possible for inspectors to require entry at times outside of ordinary business hours, which would impose onerous and expensive obligations on organisations.

CONCLUSION

Thank you again for the opportunity to provide comments. We hope that our above comments are useful to you in your preparation of the bill.

Please do not hesitate to contact the AIC at director@asiainternetcoalition.org should you require further information on the contents of this submission.

Yours sincerely,

Dr. John Ure
Executive Director
Asia Internet Coalition